Can a Stablecoin Be Collateralized by a Fully Decentralized, Physical Asset?

Maxwell Murialdo¹ Jonathan L. Belof¹

¹Lawrence Livermore National Laboratory

Published on: Jun 13, 2022
DOI: https://doi.org/10.21428/58320208.adf5637a
License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)
Abstract

Stablecoins are considered by many to be a holy grail technology for decentralized finance. These digital tokens are designed to have minimal volatility which encourages blockchain transactions, confidence, usability, and long-term smart contracts. However, to date stablecoins have always had to make tradeoffs between two desirable properties: 1) full decentralization; and 2) collateralization by a physical asset with intrinsic utility. This tradeoff stems from the conventional belief that physical assets cannot be managed in the same decentralized fashion as intangible assets (i.e., the belief that the physical assets that collateralize stablecoins must be managed by centralized, trusted custodians). In opposition to this conventional belief, we propose a new class of stablecoins that can be both fully decentralized and fully collateralized by a physical asset with intrinsic utility (electricity). We detail how statistical mechanics and information theory (via Maxwell’s demon) can be used to transfer free energy in the form of electricity between anonymous users of a decentralized network without interfacing with utility corporations, power plants, or even electrical grid networks. In turn we reveal how electricity can be used to collateralize a stablecoin such that each token can be exchanged for one kilowatt-hour (KWh) of electricity and vice versa, without any centralized authorities. In this paper we first introduce the pros and cons of three distinct classes of stablecoins. Next, we propose a new class of stablecoins that combines the advantages of fiat/asset-backed and non-collateralized stablecoins and explore the operability of this new class of stablecoins from both physics and economics perspectives. Finally, we analyze potential barriers to implementation and practical considerations relevant to this new class of stablecoins.

Keywords: Blockchain, Cryptocurrency, Energy, Electricity, Stablecoin

1. Introduction

Cryptocurrencies can broadly be divided into two categories: forms that are backed by a more conventional asset or currency, and forms that are not (i.e., collateralized vs. non-collateralized). The former category is typified by Digix (DGX), a cryptocurrency that is ostensibly backed by gold (each token is exchangeable for one gram of gold) [1]. The latter category is typified by Bitcoin, which does not claim to be backed by any conventional asset or currency [2]. Both categories of cryptocurrencies can be used to circumvent transactional frictions of traditional financial systems (e.g., no need for third party approvals, provide discretion, reduced fees). Cryptocurrencies also have
the potential to serve as a digital store of value. As a new financial technology, cryptocurrencies present a broad new landscape.

However, at present, both collateralized and non-collateralized cryptocurrencies suffer from unique caveats and potential pitfalls. To begin, cryptocurrencies that are backed by conventional assets or currencies must address storage and security concerns for their backing assets. For example, Digix ostensibly stores enough gold in its vaults to cover each crypto token it has issued. As with general physical assets, these vaults require storage space and infrastructure, and pose a risk of theft or loss. Even more critically, asset-backed cryptocurrencies entail a degree of centralization that is considered unacceptable to many in the cryptocurrency communities. The backing assets are almost never as decentralizable as the token itself. These assets are generally controlled by a single entity or a few entities, such as corporations or nation-states that act as custodians of the backing assets. Trust in these asset-backed cryptocurrencies thus requires trust in the custodians, which is antithetical to the impetus behind decentralized cryptocurrencies. (Note that trust in the custodians entails not only trust that the custodians will uphold their promises if called to do so, but also that the backing assets actually exist in the quantity/value advertised.) Real-world examples where asset-backed cryptocurrencies have failed to live up to their promises further bolster distrust. For example, Tether, which issued a cryptocurrency token that was supposed to be 100% backed by US dollars (USD), has been investigated by the New York Attorney General regarding missing funds [3]. Furthermore, at the level of a nation-state, Venezuela issued a cryptocurrency called Petro in 2018, which was supposed to be backed by the oil, gasoline, diamond, and gold reserves of the nation. However, subsequent investigation has cast doubt on the legitimacy of the alleged backing assets [4]. Moreover, if a nation-state were to issue a cryptocurrency that is directly backed by that nation’s fiat currency, there would remain risks that the nation would enact monetary policies that lead to excessive inflation.

In general, assets require credibility in order to sustain long term value. In some cases, this credibility is derived from the utility of the underlying asset (e.g., oil). However, this is not necessarily the only mechanism by which an asset can establish credibility. Cryptocurrencies that are not backed by any conventional assets or fiat currencies sidestep many of the issues associated with asset-backed cryptocurrencies. However, instead these cryptocurrencies must rely on a vital but unproven hypothesis. We note (without diving into the arguments on either side of this contentious issue) that many unbacked cryptocurrencies posit as a core hypothesis that an asset can
stably hold value purely as a result of a sufficient number of people believing that it holds value. Let us call this hypothesis the “Emergent Value Hypothesis” (EVH). This hypothesis (EVH) suggests that an asset that is initially devoid of intrinsic value can stably amass value as it amasses adopters, brand awareness, or popularity. To date, EVH-based cryptocurrencies have experienced extreme price volatility, limiting their utility. It has been argued that this price volatility may only be temporary and may be linked to a period of price discovery. However, questions around the validity of the Emergent Value Hypothesis are unresolved, and it remains to be seen whether EVH-based cryptocurrencies can and will stabilize in price.

In response to the extreme price volatility of non-collateralized cryptocurrencies like Bitcoin and Ether, stablecoins have been developed and launched. A stablecoin is a cryptocurrency that is designed to have a stable price relative to external currencies or assets. By combining many of the advantages of cryptocurrencies (such as a censorship-resistant ledger) and the advantages of a stable currency, stablecoins provide significant utility in decentralized finance. Stablecoins help to mitigate unnecessary risks to buyers and sellers, to facilitate transactions, and empower longer-term thinking and long-term smart contracts on the blockchain.

However, to date no stablecoin has been invented that is both hard pegged to a stable physical asset with intrinsic utility and fully decentralized. In this context, “hard pegged” means that each token issued is directly exchangeable for a specified quantity of a physical asset (e.g., each token can be directly exchanged for one gram of gold). A hard peg is an important standard as it eliminates additional risks that are present in soft-pegged systems.

There are three basic classes of stablecoins: fiat/asset-collateralized stablecoins, cryptocurrency-collateralized stablecoins, and non-collateralized stablecoins. The first category, fiat/asset-collateralized stablecoins, is the simplest to understand. Each of these tokens is hard pegged to a fiat currency or external asset (e.g., USD, gold). In order to maintain this peg, the fiat currency or asset is held in backup reserve to the token and is made available for direct exchange with the token at a fixed exchange rate. This type of cryptocurrency is extremely stable as long as its asset custodians can be trusted, and the backing fiat currency or asset is stable in value. A strong advantage of fiat/asset-collateralized stablecoins is that price shocks in other cryptocurrencies (or even the general cryptocurrency landscape) do not impact this class of stablecoins, no matter how large. This class of stablecoins has virtually no reliance on the unproven Emergent Value Hypothesis. The disadvantage, however, is
that to date, fiat/asset-backed stablecoins inherently require centralization at some level; trust in centralized asset custodians is necessary but also antithetical to the ethos of cryptocurrencies.

The second class of stablecoins encompasses cryptocurrency-collateralized stablecoins. As the name suggests, these stablecoins hold another cryptocurrency in collateral on the blockchain in order to fix the price of the stablecoin itself (a collateralized debt position). One prominent example of this class of stablecoins is Dai by MakerDAO [5]. Each Dai token in circulation is created as an overcollateralized loan to be paid back. The collateral is generally held in Ether (or Pooled Ether) and processing is automated by smart contracts. By adjusting the interest rate to be repaid on the loan, the quantity of Dai in circulation can be approximately controlled to maintain a soft peg of one Dai to one USD. However, this soft peg is significantly more vulnerable than a hard peg. If the price of Ether were to drop suddenly, one’s collateral could be automatically liquidated. If the price of Ether were to drop calamitously, there may not be enough locked up collateral to liquidate, and the peg could fail. Therefore, cryptocurrency-collateralized stablecoins still rely indirectly on EVH.

The third class of stablecoins, non-collateralized stablecoins, do not specifically hold any collateral. Instead, these systems use oracles to monitor the trading price of the stablecoin. This information is fed into a smart contract, which acts as a sort of automated central bank, effectively minting new tokens when the trading price increases and buying back tokens when the trading price decreases. Here the idea is to maintain stability by continual, automated adjustments of the stablecoin supply. This class of stablecoins also relies heavily on EVH.

As previously discussed, each class of stablecoins has unique pros and cons. Both non-collateralized stablecoins and cryptocurrency-collateralized stablecoins depend heavily on EVH. Fiat/asset-collateralized stablecoins, on the other hand, do not depend on EVH and have very little risk of collapse (as long as the backing asset is stable in value). Their primary downside is centralization, which requires trust in the asset custodians.

In contrast, an ideal stablecoin should have two key properties simultaneously: 1) backing by a physical asset with intrinsic utility and stable value (i.e., hard peg), and 2) full decentralization for all parts of the system. In this work, we employ statistical mechanics and information theory to detail how a stablecoin with both of these desired properties can be achieved. To the best of the authors’ knowledge, this is the first
description of a stablecoin concept that is both backed by a stable physical asset with intrinsic utility (hard pegged) and fully decentralized.

Note that the stablecoin concept proposed in this work has not yet been implemented. Full implementation of this concept will require further technological advances in the coming years, as detailed in Section 5. This work is intended as a theoretical proof of concept. This work is organized as follows. In Section 2 we describe the motivation for E-Stablecoin. In Section 3 we give a brief overview of how free energy can be transmitted as information (additional details can be found in Section 5.3 – Section 5.4 and the cited literature). In Section 4 we detail an incentive structure designed to peg the price of one E-Stablecoin token to the price of one KWh of electricity on the basis of information transfer. In Section 5 we describe several up-and-coming technologies that are likely to be important in the full implementation of E-Stablecoin and future steps that are needed. In Section 6 we discuss some implications that E-Stablecoin represents for the future of blockchain technologies.

2. Electricity-Backed Stablecoin (E-Stablecoin)

In this work we propose a new class of stablecoins whose price is hard pegged to a physical asset with intrinsic utility while still allowing for full decentralization. More specifically, the price of one token is hard pegged to the price of one KWh of electricity. We will hereafter refer to any instantiation of this newly proposed class of stablecoins as an Electricity Stablecoin (E-Stablecoin). The price peg is maintained by ensuring that each E-Stablecoin token is directly exchangeable for one KWh of electricity and vice versa; any user can mint an E-Stablecoin token with the input of one KWh of electricity (with fees) or can redeem an E-Stablecoin token in exchange for one KWh of electricity output (with fees). Crucially, there is no centralization anywhere in the system. There are no entities of authority (e.g., leadership, corporation, nation-state, centralized infrastructure, etc.) It is a trustless system.

Electricity was selected as the backing asset for E-Stablecoin due to its numerous favorable qualities. First, it is an asset that is fungible, used all over the world, and can be readily decentralized. Second, it is already used in computational processes and has abundant intrinsic demand. Third, it has held a relatively stable value over many decades. Over the past fifty years, the US price of electricity (in USD) has fallen by an average of less than one percent each year (after controlling for inflation) [6]. Moreover, over the last fifty years, scientists, engineers, and entrepreneurs have endeavored to decrease the costs of electricity production by any means possible. The stable price of electricity in the face of these pressures suggests robustness in the
value of one KWh of electricity. This stands in stark contrast to other decentralized resources such as computational power or digital data storage, whose prices have dropped exponentially over the last fifty years in accordance with Moore’s law [7]. Fourth, worldwide electricity consumption is a huge market with approximately three trillion dollars’ worth (USD) of electricity consumed annually [8]. This vast market allows ample room for additional asset storage. For comparison, in 2021 Bitcoin stored around one trillion dollars in value (on the blockchain) [9]. Over the course of several years a comparable amount of value could be stored in E-Stablecoin without significantly disrupting global electricity markets (see Section 4).

E-Stablecoin involves the effective transfer of electricity (or free energy) across decentralized nodes in a fashion that is distinct from today’s electrical grid system. E-Stablecoin does not transmit electricity through conventional power lines, but instead transfers free energy solely through the communication of information. This feature has significant utility for applications that require electricity consumption in remote locations far removed from the grid, or even for electrical grid stabilization. Nevertheless, this utility is a fortunate side effect of E-Stablecoin, not its main intent. The intended goal of E-Stablecoin is to provide a stablecoin that replicates all of the decentralized functionality afforded by Bitcoin without ever having to rely on the unproven Emergent Value Hypothesis. E-Stablecoin can eliminate all of the same transactional frictions as Bitcoin. E-Stablecoin can also attain credibility (by virtue of its backing asset and structure, not by virtue of its popularity or brand awareness). Therefore, like Bitcoin, E-Stablecoin can be used as a digital store of value.

However, E-Stablecoin is not constrained by the same structures as Bitcoin. In particular, unlike Bitcoin, the number of E-Stablecoin tokens in existence is not fixed but rather can expand or contract as needed (while maintaining constant purchasing power per token). This means that E-Stablecoin cannot be used as a speculative asset, which we see as a feature of E-Stablecoin, not a bug. In fact, just the hypothetical possibility of E-Stablecoin sheds light on the ad hoc nature of specific quirks of Bitcoin (by contrast).

3. How E-Stablecoin Works

The theory behind E-Stablecoin is built on the fact that free energy can be transferred by the transmission of information alone. It can seem daunting to try to bridge a connection between the pristine beauty, purity, and security of the ethereal digital world and the dirty, physical reality that humans must inhabit to physically survive. It is difficult to make the digital and the physical interface with one another at a
fundamental level. However, a nineteenth-century physics puzzle leads the way: Maxwell’s demon. In 1867 James Clerk Maxwell hypothesized that a “neat-fingered demon” could sort the gas molecules in a warm box by their kinetic energies, establishing a temperature gradient from a single temperature bath without expending energy [10].

This thought experiment, which seemingly violated the second law of thermodynamics, was rigorously redesigned in 1929 by Leo Szilard who posited that the demon itself must generate net entropy when measuring the particles’ temperatures [11]. In 1982, Bennett pointed out that by using “reversible computing,” the demon could measure particle temperatures and sort particles without generating any thermodynamic entropy [12]. However, in this process, information about the particles would have to be recorded in a memory bank. Accordingly, the second law of thermodynamics is not violated since converting heat into work is not the only result of the process. The process also generates “waste data” as a side product. A consideration of the various entropy contributions to the full system (including the Szilard engine, the bath, and the memory bank) shows that net entropy does not decrease, in agreement with the second law of thermodynamics.

In Szilard’s construction there is only a single gas molecule in a box. The demon can close a shutter through the center of the box, thereby trapping the molecule in a random half of the box. (Note that the demon can be replaced by a reversible computer.) If the demon knows which half of the box the gas molecule is trapped in, then it can then push a piston into the empty half of the box (unopposed). Upon reopening the shutter, the gas molecule will push on the piston to perform up to $k_B T \ln 2$ units of useful work (Equation 1). In a thermally insulated system, the particle would cool down as it performs work on the piston. However, if the Szilard engine is in thermal contact with a larger single-temperature heat bath (e.g., the earth at room temperature), then it can extract heat from the bath so that the entire process is isothermal (and conducted at the temperature of the heat bath).

$$W = -\int_{V/2}^{V} p \, dv = -k_B T \left( \int_{V/2}^{V} \frac{dv}{V} \right) = k_B T \ln 2$$

(1)

Where, $W$ is the work produced, $k_B$ is the Boltzmann constant, $V$ is the volume of the box, $p$ is the pressure, and $T$ is the temperature of the heat bath in Kelvin.
This redesign is conceptually similar to Maxwell’s demon. However, in the Szilard engine two addition facts become apparent. First, we see that exactly one bit of information (knowledge of which half of the box the particle is in) can be used to extract up to $k_B T \ln 2$ units of heat from the system and convert it into work. This one bit of information is the recorded “waste data.” Second, the measurement of the bit of information need not be concurrent with the conversion of the thermal energy into work. Once the shutter is closed and the information stored (knowledge of which half of the box the molecule is in), there is no rush to proceed. Szilard could choose to come back at any later time to convert his known bit of information into work. Furthermore, the bit of “which side of the box” information need not be stored locally (as elaborated by Hossenfelder [13]).

Recently it has been shown that a Maxwell’s demon that extracts thermal energy from a single temperature bath and converts that thermal energy into work can be physically realized [14]. Moreover, it is now understood that the “fuel” for such a Maxwell’s demon comprises the empty (preinitialized to a standard internal state) data storage space wherein the “waste data” is to be recorded. The recording of the “waste data” is unavoidable as the “waste data” is utilized in the operation of extracting the thermal energy. (Note that one cannot utilize the “waste data” without recording it in some format. Unlike in computer software, wherein a user may choose not to “save” a file, in physics, this utilized information is inherently “saved” in the state of the physical system.) Therefore, a Maxwell’s demon can continue to convert thermal energy into work until it runs out of digital memory space in which to record the “waste data” [14]. As soon as the demon runs out of memory space (i.e., fuel), it must either erase previously recorded information to free up new space or halt its process. Bennett clarified that the only thermodynamic entropy-generating step (necessarily irreversible step) in the operation of a Maxwell’s demon occurs when the stored “waste data” is erased from the memory bank [12].

Moreover, Landauer’s principle prescribes that the minimum energy that must be expended in order to erase one bit of information is $k_B T \ln 2$, where $T$ is the temperature at which the bit is erased [15]. The Szilard engine thus acts as an information engine that can extract $k_B T \ln 2$ units of work from a single temperature bath for every bit of information that it can store. However, this work ($k_B T \ln 2$) must later be repaid when it comes time to erase that bit of information from the memory bank (assuming one cannot access an infinite memory bank). The energy expenditure required to erase the bit of information thus exactly offsets the work produced by the
system. Therefore, for heat extractions from a single temperature bath, there is no net gain in free energy.

Throughout this entire process the second law of thermodynamics is preserved. This fact is counterintuitive, given that the process extracts heat from a single temperature bath (e.g., the earth) to produce work. However, in this system there are counterbalancing effects between two different types of entropy—the entropy of thermodynamic physical systems (i.e., Clausius entropy) and the entropy of information (i.e., Shannon entropy). While Clausius entropy is decreasing (as heat is converted into work), Shannon entropy is increasing (by adding entropy to the memory bank). The result is that the overall combined entropy (Clausius entropy and Shannon entropy) never decreases at any point in the process, thus preserving a generalized second law of thermodynamics. Clausius entropy can be exchanged with (or counterbalanced by) Shannon entropy. Put another way, digital information storage space can be used as an indirect store of thermodynamic free energy! This process is elaborated on in Section 5.3.

This thought experiment paves a theoretical path forward for “storing” and “transmitting” electrical free energy (as a backing asset) in a fully decentralized cryptocurrency network. The first step is to detail how free energy (or electricity) can be transferred between two remote parties (Alice and Bob) solely by the transmission of information between those two parties. We have outlined a protocol to do so below.

### 3.1 Protocol A

Protocol for transferring free energy between two remote parties (Alice and Bob) by the transmission of information only:

1. Alice connects a Szilard engine to a large thermal mass at a single temperature. For example, Alice may use the earth (at room temperature) as the thermal mass.
2. Using reversible computing, Alice extracts heat from the thermal mass and converts that thermal energy into work (electricity). This necessarily produces “waste data” which must be stored locally. Note that the thermal mass is assumed to be sufficiently large such that extracting a moderate amount of heat from it does not appreciably change its temperature. Alice can use the generated electricity locally to perform daily tasks.
3. Alice can continue to extract thermal energy and convert it into work (or electricity) until her local data storage hard drive is full of “waste data”. At this point, Alice must clear her data storage hard drive in order to be able to extract additional thermal
energy. However, if Alice were to erase her “waste data” locally, she would have to expend all of the free energy that she previously extracted (by Landauer’s principle), assuming that all processes are conducted at a single temperature (room temperature). Instead, Alice can outsource her data erasure process to Bob (who is at a physically distant location from Alice). This is done by reversibly transferring the “waste data” on Alice’s hard drive to available storage space on Bob’s hard drive (see Section 5.4 for more details). The result is that Alice’s data storage space is reset to its initial (empty) condition while Bob’s previously empty data storage space is now filled with Alice’s “waste data.” This outsourcing process can in theory be done without expending any free energy. Here counterfactual communication channels can be established between Alice and Bob in order to transmit information between remote locations without transferring any matter/energy (or physical particles) through the intervening space.

4. In the final step, Bob expends free energy at his location in order to erase Alice’s “waste data” from his hard drive (in accordance with Landauer’s principle). The net effect is that Bob has locally put \( \sim z \) KWh of electricity into the system and Alice has locally extracted \( \sim z \) KWh of electricity from the system (assuming high efficiency processes). This is effectively a transfer of free energy from Bob to Alice (who are physically separated). Moreover, only information (no matter/energy) is transmitted between Alice and Bob. We note that no matter/energy is ever transferred between Alice and Bob. Alice extracts thermal energy (locally) which is converted into work (or electricity) and used locally. Eventually, that work (through friction) will be converted back into thermal energy at Alice’s location, in accordance with the first law of thermodynamics.

3.2 Protocol B

Protocol A (described above) can in turn be used as the basis for an E-Stablecoin network, wherein the price of each E-Stablecoin token is pegged to the price of one KWh of electricity. A broad overview of the operation of the E-Stablecoin network is presented below in Protocol B:

1. Alice (now representative of any user of the E-Stablecoin network) connects a Szilard engine to a large thermal mass at a single temperature. Alice extracts thermal energy and converts it into one KWh of electricity (along with “waste data” which she stores locally via reversible computing). Alice uses the extracted electricity locally to perform daily tasks.
2. For the price of one E-Stablecoin token plus a fee, Alice outsources her “waste data” erasure process to a decentralized data storage cloud (D). In this exchange a smart contract destroys the E-Stablecoin token(s) that Alice paid for this service. The decentralized data storage cloud is housed across a network of privately owned (decentralized and anonymous) reversible computers (see Section 5.1 for more details). The private owners of these reversible computers are incentivized to share their storage space with the E-Stablecoin network in exchange for fees. The specific fee due to each contributor of data storage space is computed and dispersed automatically by a smart contract (see Section 5.1).

3. Bob (now representative of any user of the E-Stablecoin network contributing storage space to D) can expend his own electricity (locally) to erase the “waste data” outsourced to his privately owned hard drive. For this service Bob is awarded one E-Stablecoin token plus a fee. This transaction is automatically mediated by a smart contract. The smart contract creates new E-Stablecoin token(s) to pay to Bob for his services rendered.

4. The fee structure is regulated with a transparent, automated smart contract based on an estimate of the percentage of D that is currently empty (see Section 4).

4. Economics and Incentive Structures

E-Stablecoin is designed to fulfill the same functionality as Bitcoin without relying on the Emergent Value Hypothesis. Like many other cryptocurrencies, Bitcoin can remove transactional frictions and middlemen from financial transactions. However, Bitcoin has the potential to go far beyond this functionality as a long-term store of value. In this role, many have likened Bitcoin to a digital form of gold (that is easier to store, secure, transport, and transfer). From its ledger inception in 2009 through 2021, Bitcoin expanded to a market cap of roughly US $1 trillion [9]. This is tantamount to saying that approximately one trillion dollars’ worth of value worldwide has been stored in the asset form of Bitcoin (as compared to approximately ten trillion dollars’ worth of value that has been stored in the asset form of gold) [16]. Unlike gold, Bitcoin does not have a consistent track record for storing value over thousands of years—Bitcoin is far too young for these credentials. However, many nonetheless believe that Bitcoin will maintain value by virtue of its popularity-borne credibility. This belief is consistent with EVH.

E-Stablecoin, on the other hand does not rely on EVH. Instead, its credibility and value as an asset derive from the utility of its backing asset (electricity). The price of each E-Stablecoin token is hard pegged to the price of one KWh of electricity. This is
maintained by ensuring that one E-Stablecoin token can always be exchanged (cashed in) for one KWh of electricity (plus fees). Likewise, the opposite conversion is equally valid; one KWh of electricity can always be used to mint one new E-Stablecoin token (plus fees). Furthermore, this process is fully decentralized so that no authority can intervene in the creation or cashing in of E-Stablecoin tokens.

Once E-Stablecoin tokens are created in this decentralized fashion, they can be transacted with between individuals directly, using smart contracts, or through cryptocurrency exchanges. Like Bitcoin, they can also be used as a store of value.

The minting of new E-Stablecoin tokens requires the consumption of electricity. Will electricity markets be able to stably bear the new demands placed on them (as electricity is consumed to mint new E-Stablecoin tokens as stores of value)? Ostensibly, yes. Each year approximately three trillion dollars’ worth of electricity is consumed globally [8]. In order to mint one trillion dollars’ worth of E-Stablecoin tokens over the course of twelve years (comparable to Bitcoin), this action would only increase global electricity demand by an average of 2.8%. For comparison, the electricity consumption worldwide from 2010 to 2018 increased by roughly 2.8% per year [17]. Moreover, studies have suggested that long-term electricity supply elasticities are in the range of 0.98-2.7 [18] [19]. This range suggests that electricity markets should be able to compensate their supply to account for the slight increase in demand associated with E-Stablecoin token minting, without drastically altering prices.

Additionally, daily averages for global electricity consumption should not pose a bottleneck for E-Stablecoin token to electricity conversions. An individual who chooses to cash in E-Stablecoin tokens in exchange for electricity may choose to use the electricity for personal consumption, store the energy locally, or sell the electricity to the local grid (similar to residential solar power producers). Each of these options has a limited capacity. For example, cashing in one billion dollars’ worth of E-Stablecoin tokens for an equivalent value in KWh of electricity (over a small timeframe and in an isolated location) may pose an electricity consumption conundrum. However, on average, approximately eight billion dollars’ worth of electricity is consumed daily across the globe [8]. Significant quantities of E-Stablecoin tokens could thus be cashed in (converted into electricity) globally over reasonable intermediate timeframes. More importantly, however, large quantities of E-Stablecoin tokens do not need to be minted or cashed in for electricity on a daily basis in order to maintain the hard peg. Most transactions will occur by exchanging E-Stablecoin tokens between wallets and exchanges, as is the case for Bitcoin. The mere fact that each E-Stablecoin token can
always be cashed in for electricity, coupled with a moderate rate of users cashing in, is sufficient to maintain the hard peg of one E-Stablecoin token to one KWh of electricity.

### 4.1 Potential Failure Modes and Deterrence Strategies

There are two main potential failure modes by which the exchange of E-Stablecoin tokens for electricity could be disrupted and the hard peg of one E-Stablecoin token to one KWh of electricity would fail. Both potential failure modes are tied to \( \phi \), the fraction of total data storage space in D that is presently in use to store “waste data.” (Note that D is the decentralized data storage cloud supporting E-Stablecoin, and \( 0 < \phi < 1 \)).

\[
\phi = \frac{O}{O + U}
\]

Where \( O \) is the quantity of occupied storage space in D, and \( U \) is the quantity of unoccupied storage space in D.

The first potential failure mode could occur if the demand for E-Stablecoin tokens were too high, and D utilization reached zero percent of its total capacity (i.e., D contains no additional “waste data” to erase, \( \phi = 0 \)). In this scenario, users would no longer be able to mint new E-Stablecoin tokens (although the destruction of E-Stablecoin tokens by cashing them in for electricity could continue). This scenario could create a scarcity of E-Stablecoin tokens (greater demand than supply), driving the exchange price of one E-Stablecoin token above the price of one KWh of electricity. The resulting price increase could in turn drive further demand to mint new E-Stablecoin tokens and reduce demand to cash in E-Stablecoin tokens for electricity. This feedback loop could lead to a massive price spike, decohering the price of the E-Stablecoin token from the price of electricity.

The second potential failure mode could occur if D were to become fully utilized and could not accommodate the storing of any additional “waste data” (\( \phi = 1 \)). If this were to occur, then users would not be able to cash in E-Stablecoin tokens for electricity. New E-Stablecoin tokens could be minted (with the input of electricity), but no E-Stablecoin tokens could be cashed in (destroyed in exchange for electricity). The overabundance of E-Stablecoin tokens in circulation would be expected to drive the exchange price of the E-Stablecoin token down (below the price of one KWh of electricity). The resulting price drop could in turn drive further demand to cash in E-Stablecoin tokens for electricity and reduce demand to mint new E-Stablecoin tokens.
(further reducing the E-Stablecoin token exchange price). This could potentially lead to a feedback loop induced panic (not unlike a run on the banks) and the ultimate price collapse of E-Stablecoin tokens. It is important to note that if D were inherently static or growing in size, this second failure mode could not occur. If the size of D were static, for instance, the number of E-Stablecoin tokens in circulation could be maintained precisely in step with the available data storage capacity necessary to convert each of those E-Stablecoin tokens into one KWh of electricity. In this hypothetical scenario, each E-Stablecoin token could be exactly collateralized with a commensurate quantity of available data storage capacity by enforcing that E-Stablecoin tokens only be created by the erasure of data or addition of commensurate data storage capacity to D. In this hypothetical scenario, if \( \phi = 1 \), it would also imply that no E-Stablecoin tokens are currently in circulation. No one would be left holding the bag, upset that their E-Stablecoin token could not be converted into one KWh of electricity, since all E-Stablecoin tokens would have already been cashed in (destroyed). Therefore, for a static D, this is not a legitimate failure mode.

However, due to the decentralized nature of the E-Stablecoin data storage cloud, D is not static and can grow or shrink in size in accordance with users’ decentralized actions. It would therefore be possible at any given moment for there to exist more E-Stablecoin tokens in circulation than could be cashed in at a one E-Stablecoin token to one KWh of electricity ratio. The goal of E-Stablecoin is to serve as a stablecoin whose price is pegged to the price of one KWh of electricity (not to enable speculation). Therefore, deterrence strategies must be incorporated into the E-Stablecoin network in order to prevent either potential failure mode (too much or too little available capacity in D).

One way to prevent these failure modes is to introduce economic pressures (in the form of smart contract-mediated fees) that help to ensure that \( \phi \) remains close to \( \Omega \) (where \( \Omega \) is the optimal fractional usage of D in order to maintain stability). Under this system, each time Alice cashes in an E-Stablecoin token for one KWh of electricity by outsourcing her “waste data” to D, she must pay an additional variable fee, \( x \), (also in E-Stablecoin). Likewise, whenever Bob accepts one KWh equivalent of data from D for erasure, he will receive one E-Stablecoin token plus a variable fee, \( y \), (in E-Stablecoin). Enforcement of the fees is mediated using a preset and transparent smart contract (see Section 5.1). The values of \( x \) and \( y \) are variable and depend on the current number of E-Stablecoin tokens in existence, \( M \), and on \( \phi \).
When $\phi < \Omega$, the values of both $x$ and $y$ decrease as $\phi \to 0$. In this domain, the demand to mint E-Stablecoin tokens by expending electricity to erase “waste data” from D has exceeded the demand to cash in (destroy) E-Stablecoin tokens in exchange for electricity. This demand mismatch is counterbalanced by the variable fees. As $x$ decreases, parties have increasing incentive to cash in E-Stablecoin tokens for electricity by outsourcing “waste data” to D. Likewise, decreasing $y$ diminishes the incentive for parties to mint new E-Stablecoin tokens by erasing “waste data” from D. These imposed economic pressures help to push $\phi$ back towards an optimum value of $\Omega$.

It is furthermore important to elucidate the incentive structure used to encourage parties to contribute their private, decentralized data storage capacity to D. Any party (i.e., Bob) can only receive E-Stablecoin tokens from the smart contract in exchange for accepting outsourced “waste data” to his privately owned data storage device. Bob may then choose to expend electricity to erase the “waste data” on his storage device at his leisure; this action (erasure) is not mandated or monitored by the smart contract. Instead, the smart contract allocates “waste data” to the available storage space in D at random. Bob cannot mint E-Stablecoin tokens at an arbitrarily high rate. He can only mint E-Stablecoin tokens in proportion to the rate at which the smart contract allocates (outsources) “waste data” to Bob’s personal data storage device. In this case, Bob’s personal storage devices are a part of D. Let the ratio of the available (empty) data storage space that Bob’s personal devices contribute to D, $U_B$, divided by the total available (empty) digital storage space in D, $U$, (both at a single instant in time) be denoted by the variable $\lambda(t)$ (Equation 3). Accordingly, the average maximum rate at which Bob can mint new E-Stablecoin tokens, $r$, is given by Equation 4.

$$\lambda(t) = \frac{U_B}{U}$$

$$r = \omega(t) \lambda(t)$$

Where $\omega(t)$ is the rate at which E-Stablecoin tokens are being cashed in on the E-Stablecoin network at a given time.

As seen in Equation 4, Bob can increase the rate at which he can mint E-Stablecoin tokens by increasing the data storage space that he is contributing to D. In general, it will be profitable for Bob to contribute data storage space to D and to input electricity
to erase any data outsourced to his storage space as quickly as possible if the following inequality is true:

\[ rt(1 + y)(P_E) \geq rt \left( P_{KWhl} \right) \left( \frac{1}{\nu} \right) + c_1 + c_2 \]  

(5)

Where \( P_E \) is the trading price of an E-Stablecoin, \( P_{KWhl} \) is Bob’s local price for one KWh of electricity, \( \nu \) is the energetic efficiency of electricity to E-Stablecoin token conversion, \( t \) is the time over which Bob contributes data storage to D, \( c_1 \) is the operational cost of Bob’s contributed data storage over time \( t \), and \( c_2 \) is the amortization cost of Bob’s contributed data storage over time \( t \).

As seen in the inequality above, the profitability that Bob can achieve by contributing data storage space to D and erasing data from his personal data storage space as quickly as possible depends heavily on the fee value, \( y \). It also depends on the local cost of electricity for Bob (\( P_{KWhl} \)). Bob has two independent choices to make: Step 1) contribute data storage space to D at any given time; and Step 2) input electricity to erase “waste data” outsourced to his data storage space at any given time. While Step 2 cannot be achieved without first completing Step 1, there is no mandatory timeframe in which Step 2 must be completed after completing Step 1. For example, Bob could receive “waste data” to his personal data storage at time \( t_1 \) and choose to wait until the local cost of electricity drops at time \( t_2 \) (e.g., on a diurnal cycle) before erasing the “waste data” from his hard drive. Alternatively, Bob may pause Step 2 if the value of \( y \) drops too low. Note that it would not necessarily behoove Bob to erase previously accepted “waste data” from his personal drive during this pause, as erasure would require the expenditure of electricity and may not be profitable. Bob’s decision to complete Step 2 after completing Step 1 depends on both the global, time-dependent value of \( y \), and the local, time-dependent cost of electricity. Moreover, temporal variations in the local cost of electricity may become more pronounced as intermittent renewable energy sources (e.g., wind and solar) are added to local grids. It is therefore anticipated that distinct parties located in different regions across the globe will algorithmically choose to complete or pause Step 2 at different times so as to maximize their profits (e.g., based on the immediate availability of low-cost renewable energy from wind or solar).

When \( \phi > \Omega \), the values of both \( x \) and \( y \) increase as \( \phi \to 1 \). In this domain, the demand to cash in E-Stablecoin tokens (destroying the E-Stablecoin tokens in exchange for
electricity) has exceeded the demand to mint new E-Stablecoin tokens by erasing “waste data”. Once again, this demand mismatch is counteracted by the variable fees. As $x$ increases, Alice is less incentivized to cash in E-Stablecoin tokens, and as $y$ increases, Bob is more incentivized to mint new E-Stablecoin tokens. If Bob is already expending electricity to mint new E-Stablecoin tokens at a maximal rate (given his $\lambda(t)$), then he is incentivized to add additional data storage to $D$ in order to increase his $\lambda(t)$ and receive a larger quantity of “waste data” to erase per second. All of these economic pressures help to force $\varphi$ back towards an optimal value of $\Omega$.

The functions $x$ and $y$ can be modeled as follows.

Let us define the surplus rate, $R_s$, as the rate at which E-Stablecoin tokens are minted minus the rate at which E-Stablecoin tokens are cashed in (destroyed). Let the surplus rate elasticity, $R_e$, be defined by Equation 6.

$$R_e = \frac{\partial (R_s)}{\partial y}$$

(6)

Let the target surplus rate, $R_T$, be a function of $\varphi$ as per Equation 7. The target surplus rate defines the ideal surplus rate to be aimed for by the operations of the smart contract.

$$R_T = f(\varphi)$$

(7)

Note: When $\varphi > \Omega$, $R_T$ is positive. When $\varphi < \Omega$, $R_T$ is negative.

We define the base fee, $\beta_f$, as a function of $R_s$, $R_e$, and $R_T$ (Equation 8). Note that $R_s$ and $R_e$ have values that are measured by smart contract and depend on the operation of the smart contract in response to the decentralized actions of the E-Stablecoin network users. $R_T$ is a predefined function of $\varphi$.

$$\beta_f = f(R_s, R_e, R_T)$$

(8)

We additionally define the base fee correction term, $\beta_c$, as a function of $\varphi$, as well as the number of E-Stablecoin tokens in existence, $M$, and the optimal number of E-Stablecoin tokens, $N$ (defined below). The base fee correction term allows for adjustments to the number of E-Stablecoin tokens in existence, to ensure that each E-Stablecoin token is fully collateralized by one KWh of electricity (via available data
storage space in D). In general, $B_c$ will be close to zero and $x \approx y$, so that the number of E-Stablecoin tokens in existence remains approximately constant. The number of E-Stablecoin tokens in existence is only adjusted (via $B_c$) in response to changes in the available capacity of D.

$$
\beta_c = f(\varphi, \frac{M}{N})
$$

(9)

The fees, $x$, and $y$, are accordingly defined as follows:

$$
x = \beta_f - \beta_c
$$

(10)

$$
y = \beta_f + \beta_c
$$

(11)

The trading price of an E-Stablecoin token can make small excursions above and below the price of one KWh of electricity. However, considerable incentive pressures (via variable fees) ensure that the price remains pegged to within a small range, $\varepsilon$, of the price of one KWh of electricity.

Based on Equation 6 - Equation 11, it is theoretically possible for the number of E-Stablecoin tokens in existence to vary between zero and $Dk_B T ln 2$ (where $D$ is the size of the decentralized data storage cloud in bits, and $k_B$ is the Boltzmann constant in units of KWh per Kelvin). As $\varphi \rightarrow 1$, the number of E-Stablecoin tokens in existence, $M$, approaches zero. Conversely, as $\varphi \rightarrow 0$, $M \rightarrow Dk_B T ln 2$. Nonetheless, at every timepoint, every E-Stablecoin token is fully collateralized by one KWh of electricity (or very close to it). That is to say that if the system were frozen at any arbitrary moment in time and fully liquidated, each E-Stablecoin token in existence would be matched by one KWh of electricity (available as data storage in D). However, the fee-based incentive pressures are designed to prevent either extreme and should instead maintain $M$ near the optimal number. The optimal number of E-Stablecoin tokens in existence, $N$, occurs when $\varphi = \Omega$. $N$ is given by Equation 12.

$$
N = \Omega(U + O)(T ln 2) \left(3.84 \times 10^{-30}\right)
$$

(12)

Where $U$ and $O$ are measured in bits, and $T$ is the temperature in units of Kelvin.

In many ways the E-Stablecoin, smart contract-mediated, variable fee system resembles non-collateralized stablecoins that use transparent algorithms implemented
by smart contracts to control the token supply. In the case of E-Stablecoin, the smart contracts implement variable fees to keep $\varphi \approx \Omega$ and likewise $M \approx N$. This fee structure depends on $\varphi, M, N, R_s$, and $R_e$, and automatically adjusts as D grows or shrinks in size. We note that the total value that can be stored in the form of E-Stablecoin tokens, $V$, is limited by the size of D (Equation 13).

$$V \leq P_E(U + O)(Tln2) \left(3.84 \times 10^{-30}\right)$$ (13)

We additionally note that while the short-term fee structure depends on $\varphi, M, N, R_s$, and $R_e$, and Equation 6 – Equation 11, it may be advantageous to allow some of the fixed parameters implicit in Equation 6 – Equation 11 to drift very gradually on a timescale of several years. An additional long-timescale recalibration term could slowly shift how the free parameters define the fee structures for $x$ and $y$. This long-timescale calibration term could help the E-Stablecoin network to account for and adjust to long-timescale technological advances that could shift the efficiencies, elasticities, or profitabilities of minting or cashing in E-Stablecoin tokens.

The E-Stablecoin network combines the advantages of non-collateralized stablecoins and fiat/asset-collateralized stablecoins. It is similar to non-collateralized stablecoins in that E-Stablecoin uses transparent smart contracts to mediate stable monetary policy. However, it is also similar fiat/asset-collateralized stablecoins in that each E-Stablecoin token in existence is fully collateralized by a physical asset with broad intrinsic utility. Combined, these advantages translate into a stablecoin that is both fully decentralized and secured by a real-world asset.

### 4.2 Profitability and Arbitrage

As per Equation 5, the rate at which cashing in occurs on the E-Stablecoin network partially determines the return on investment for an individual contributing data storage space to D. While we expect that the cost of adding new, blank data storage space will always exceed the cost of expending electricity to erase an equivalent amount of existing but filled data storage space, a high cycle rate (of accepting and erasing “waste data”) increases the return on investment (and therefore the incentive) for an individual to contribute data storage space to D.

Some advantages that could drive usage of the E-Stablecoin network for electricity transfer (e.g., minting and cashing in of E-Stablecoin tokens), and therefore a high cycle rate, are natural opportunities for arbitrage. At present the price of electricity varies drastically by country and even by region. Germany has the highest average...
electricity price at ~$0.36 per KWh; for comparison, in Qatar the price of electricity is as low as ~$0.03 per KWh [20][21]. A savvy investor may therefore take advantage of this arbitrage opportunity by minting E-Stablecoin tokens in Qatar and cashing in these same E-Stablecoin tokens in Germany, where the same KWh of electricity could be sold back to the grid at a higher price point. Globally, the prices of electricity are affected by distinct regulatory policies including taxes and subsidies. The advent of E-Stablecoin and associated arbitrage opportunities would likely help to push the price of electricity in most nations towards a single global average. Instead of having distinct local pricing structures, electricity would likely be pushed towards a single worldwide price or a small range of prices (like other commodities such as oil and gold). However, it is nonetheless likely that the production costs of electricity will continue to vary by country and by region based on local factors such as local demand, the price of labor, local infrastructure, natural resources, and even the local weather. Therefore, location-based opportunities for arbitrage using E-Stablecoin may continue to exist.

Other potential sources of arbitrage that could drive E-Stablecoin usage for energy transfer are diurnal and/or seasonal fluctuations in the price of electricity. It is common for electricity prices to fluctuate by up to ten percent depending on the month and time of day [22]. A savvy investor may attempt to incorporate predictable diurnal or season pricing cycles into an E-Stablecoin arbitrage model.

Finally, we consider the possibility of using temperature differences at different locations around the globe as a source of arbitrage. The decentralized usage and exchange of E-Stablecoin tokens makes this a factor to consider. For example, if Bob could mint an E-Stablecoin token in a cold location, but then cash in the E-Stablecoin token in a hot location by extracting energy (using a Szilard engine) from the ambient temperature surroundings, Bob would effectively have created a remote heat engine operating between hot and cold locations on Earth. For reference, the coldest temperature measured on Earth was 178 K in Antarctica [23]. The hottest temperature measured on Earth was 327 K, measured in Death Valley, California [24]. Per Equation 14 below, operating a heat engine between these two temperatures \( T_{\text{hot}} \) and \( T_{\text{cold}} \) at the maximal (Carnot) efficiency, \( \eta \), could result in a 45.6% efficient conversion of heat to work. Therefore, this form of arbitrage is hypothetically possible, but many other factors would need to be taken into consideration to determine its profitability.
\[
\eta = \frac{\text{Net Work}}{Q_H} = \frac{k_B T_{\text{hot}} \ln n_2 - k_B T_{\text{cold}} \ln n_2}{k_B T_{\text{hot}} \ln n_2} = \frac{T_{\text{hot}} - T_{\text{cold}}}{T_{\text{hot}}} = \frac{149}{327}
\]

Where \(Q_H\) is the heat transferred.

5. Practical Considerations

Here we consider the practicality of five technologies that are important for the smooth and efficient operation of the E-Stablecoin network.

5.1 Smart Contracts and Decentralized Data Storage Cloud

For the E-Stablecoin network, smart contracts are used to control the creation, destruction, and distribution of E-Stablecoin tokens. Furthermore, smart contracts manage the decentralized data storage cloud, D, associated with the E-Stablecoin network. Herein we provide a high-level overview of how the system operates but leave further development and implementation of the E-Stablecoin network as future work. The smart contracts may be implemented on an existing blockchain such as Ethereum [25] or Cardano [26]. (Note that the E-Stablecoin network should be implemented on a proof of stake consensus mechanism blockchain in order to avoid the energy costs associated with a proof of work consensus mechanism.)

To begin, smart contracts must manage the decentralized data storage cloud, D. Decentralized data storage networks are comprised of distributed networks of private data storage hard drives. The goal is to remove centralized governing authorities and their control over file storage and sharing (as one might find for cloud storage offered by private corporations and hosted on centralized server farms). Popular implementations of decentralized storage networks include Filecoin [27] (using the Interplanetary File System protocol), Sia [28], Storj [29], and Swarm [30]. The decentralized data storage network of E-Stablecoin works in a similar fashion to these other implementations, with the exception that in the case of E-Stablecoin the storage space must be compatible with reversible computing. Additionally, long-term data preservation is not a goal for E-Stablecoin’s decentralized data storage cloud. Most data in D are “waste data” and therefore if these data are lost or corrupted, little damage is done. Accordingly, in general the data in D are not stored redundantly, and no centralized data recovery or data rectification process is necessary.

Using D, Alice can effectively outsource her “waste data” to a remote hard drive owned and operated by Bob. (Note that Bob is a participant who has contributed space.
on his personal hard drive to D, for a profit incentive.) The result is that Alice’s local data storage hard drive is returned to its initial, empty state, while Bob’s initially empty data storage hard drive becomes populated with Alice’s “waste data” (all while expending little to no energy—see Section 5.4 for further details). In this process, smart contracts managing D must complete multiple subtasks.

First, Alice will broadcast the quantity of information that she is seeking to outsource. Likewise, each Bob node (representing different participants contributing storage space to D) on the network will broadcast their available storage capacities. Smart contracts will match each Alice node to one or more Bob node(s) for data transfer. The specific Bob node(s) that are to receive the data are selected at random (by smart contract) such that the probability of any particular Bob node receiving data is proportional to the $\lambda(t)$ of that Bob node. Alice will then reversibly outsource her “waste data” to the selected Bob node(s) (see Section 5.4). A smart contract will quantify the amount of information that Alice transfers and will validate that it matches the amount of data that Alice initially broadcast. Once each Bob has received the data, he will (in an automated fashion) apply a transformation to the data and thereby derive a set of instructions that, when applied within Alice’s reversible computer, will reset Alice’s local data storage drive to its initial, empty state with little to no energy expenditure (see Section 5.4). Next, Bob will send these instructions to Alice. A smart contract will validate that Bob’s instructions are legitimately derived.

This validation can be carried out using zero-knowledge proofs. To do so, Alice will first divide her “waste data” into subsets and randomly select a finite number of subsets for validation purposes. She will then compute the instructions that would be necessary to reset (erase) each of the selected subsets. Next, she will concatenate each set of computed instructions with an identifier of that subset and take a cryptographic hash of those concatenations. Finally, she will upload the computed cryptographic hash values to a smart contract (in an encrypted format). Likewise, for each “waste data” subset for which Bob computes erasure instructions, he will concatenate his computed instructions with the appropriate subset identifier. Bob will then take a cryptographic hash of the concatenation and upload the hash values to the smart contract. (Here it is assumed that the data is subdivided into batches in a standardized fashion with standard identifiers.) The smart contract will then use zero-knowledge proofs to validate whether or not all of the hash values uploaded by Alice can be found within the set of hash values uploaded by Bob. If true, then Bob has passed the validation test.
A smart contract will also mediate the E-Stablecoin transactions for the aforementioned services rendered. The smart contract will charge Alice E-Stablecoin token(s) in accordance with the quantity of “waste data” that she outsources and the applicable fees. This is done before Alice is allowed to receive erasure instructions from Bob. The smart contract will destroy the E-Stablecoin token(s) charged from Alice. The smart contract will also create and pay E-Stablecoin token(s) to Bob in exchange for his services rendered in accordance with the quantity of “waste data” that he accepts and the applicable fees. Bob will only receive (E-Stablecoin) payment from the smart contract after he has passed the validation test. Note that the validation steps (taken by Alice and Bob) need not be conducted reversibly. Here it is assumed that the quantity of information calculated, stored, transmitted, and erased in association with the validation steps is negligible compared to the total quantities of information being transferred. This follows, for instance, from the fact that a very large data file can be uniquely identified by a cryptographic hash with a very small number of bits.

A smart contract is also tasked with setting the variable fees ($x$ and $y$) based on the E-Stablecoin network parameters: $\phi$, $M$, $N$, $R_s$, and $R_e$. This is performed in accordance with Equation 6 - Equation 11. Determining $M$ is straightforward: it is simply the difference between the number of E-Stablecoin tokens created by the smart contract and the number of E-Stablecoin tokens destroyed by the smart contract. Both $R_s$ and $R_e$ can be determined in similar straightforward manners. Determining $\phi$ and $N$ on the other hand, requires knowledge of the total amount of digital storage space in $D$, both the occupied space, $O$, and the empty space, $U$.

A smart contract can use auditing to determine approximately how much free (empty) data storage space is available in $D$. Note that determining approximate (though not exact) values of $\phi$ and $N$ are sufficient for the E-Stablecoin network to function smoothly. Upon adding a node to $D$, Bob is required to declare how much data storage space he is committing to $D$ and to deposit collateral (in E-Stablecoin and proportional to the quantity of data storage space committed) to be held by the smart contract. Bob is allowed to increase or decrease the amount of storage space committed to $D$ at will (and increase or decrease his collateral commensurately) by first declaring his intentions (to the smart contract).

However, the smart contract will also audit Bob’s declared committed data storage space on a random schedule. This is necessary because there exists an incentive for Bob to cheat and to declare more storage space than he has actually committed. For
example, by fraudulently declaring additional space, Bob could induce the smart contract to serve him more “waste data” to process than his fair share, which could increase the profitability of his endeavors per Equation 4 – Equation 5. In order to discourage this deception, Bob will be punished (by losing collateral) if his deception is uncovered by an audit. If Bob is currently under audit, he must first provide the required validation data (to the smart contract) before adjusting the amount of storage space he has committed to D. Otherwise, he will be punished by losing collateral.

The auditing process can be implemented by smart contract using a proof of space-type protocol. A proof of space protocol ensures that Bob has allocated a known quantity of disk space (data storage) to a verifiable task provided by the smart contract [31]. For example, in one implementation, Bob may be asked to construct a labeling of a hard-to-pebble graph (requiring a known amount of data storage space). The verifier can later ask Bob to open random locations within the labeling. If Bob can provide the verifier with the requested validation data, then he has passed the verification and has demonstrated that he is presently storing the required quantity of data. Proof of space was designed as a more energy efficient alternative to the proof of work consensus protocol employed by Bitcoin. Similar protocols such as proof of space-time [32], proof of capacity [33], proof of retrievability [34], and proof of replication [35] represent improvements on the proof of space concept and have been implemented in blockchain applications such as Burstcoin [36], Chia [37], and Filecoin [27].

As soon as Bob declares an amount of storage space that he is committing to D, he will be required to store proof of space-type data of that same number of bits (filling up the data storage space that Bob has committed to D). The smart contract will ask for verification that this data is being correctly stored using an audit process initiated at randomly selected timepoints. If during any audit Bob cannot provide proper verification, he will be punished by losing collateral (mediated by smart contract). As “waste data” is distributed to Bob for erasure, a smart contract will initiate the reversible removal (erasure) of some of the proof of space-type data from Bob’s hard drive. The data removed is commensurate in quantity to the data added, so that Bob’s declared space is always fully filled, either by “waste data” or by proof of space-type data. Note that data can be reversibly erased from Bob’s hard drive if that information is already stored redundantly elsewhere (see Section 5.4). In this implementation, the proof of space-type data is stored redundantly across multiple distinct Bob nodes (operated by distinct users).
For the purposes of calculating Bob’s specific $\lambda(t)$, the empty space contributed by Bob to D, $U_B$, is defined as the quantity of proof of space-type data that Bob is currently storing. After deleting the “waste data” that has been outsourced to him and re-freeing additional storage space, Bob will broadcast his additional storage capacity to the smart contract. The smart contract will once again fill this space with either “waste data” or proof of space-type data. It is therefore generally most rational for Bob to broadcast his additional storage space (upon data erasure) as quickly as possible (as this increases his $\lambda(t)$). We additionally note, however, that Bob is only allowed to delete “waste data” after being given permission to do so by the smart contract. Failure to wait for this smart contract-mediated permission could result in the loss of collateral or compensation. This feature allows the smart contract to build in delays to the erasure process.

Thus, $\varphi$ and $N$ can be estimated using smart contract auditing as these parameters depend on $O$ and $U$. The parameter $O$ (the occupied digital storage space in D) is determined as the difference between the amount of “waste data” that has been distributed and the amount of “waste data” that has been reported as deleted by the various Bob nodes. The parameter $U$ (the unoccupied digital storage space in D) is estimated from the total announced digital storage space committed to D by the various Bob nodes (and validated with auditing).

Finally, we note that the E-Stablecoin collateral, $C_l$, that Bob must lock away in order to contribute storage space to D is dictated by Equation 15.

$$C_l = q \left( U \right) \left( \lambda(t) \right) (Tl \ln 2) \left( 3.84 \times 10^{-30} \right)$$  \hspace{1cm} (15)

Where $q$ is the collateralization rate ($0 < q < 1$).

As long as $q$ is less than one, the quantity of E-Stablecoin in existence ($M$) can potentially be expanded indefinitely with the addition of storage space to D, per Equation 16. This model bears some similarity to fractional-reserve banking and can be thought of as a recursive process wherein $M$ can be expanded iteratively by the addition of collateralized data storage space to D in $n$ successive iterations.

$$M \leq J \left( 1 + \frac{1}{q} \right)^n$$  \hspace{1cm} (16)
Where \( J \) is the starting quantity of E-Stablecoin in existence at the inception of the E-Stablecoin network.

5.2 Counterfactual Communication

It has previously been established that there is no theoretical minimum energy expenditure required to transmit a bit of data from point A to point B (along either classical channels or quantum channels) \[38\]. As an overidealized example, one could envision data transfer by a frictionless billiard ball launched from point A to point B where its kinetic energy is completely recovered at point B. Alternatively one could envision the transmission of a photon from point A to point B wherein the photon energy is fully recovered at point B (through reabsorption). Either technique could be used to transmit digital information while dissipating only a finite quantity of energy that can in theory be made arbitrarily small. However, these and other similarly overidealized examples still entail the transfer (or contact) of matter/energy (or physical particles) from point A to point B.

In order to ensure that E-Stablecoin remains as generalizable as possible, it would be advantageous to transmit data across decentralized nodes in the E-Stablecoin network in a manner that does not transfer matter/energy from point A to point B. This form of data transmission (counterfactual communication) would prevent, for instance, the undue accumulation or depletion of matter/energy at different nodes throughout the system. Counterfactual communication also holds the potential to enable the efficient communication of information between remote locations while dissipating as little free energy as possible. Reducing “frictional costs” is essential to the efficient and effective operation of the E-Stablecoin network. (Note that in the E-Stablecoin network, free energy (or electricity) is transmitted between remote, anonymous users as pure information, without requiring an electrical grid or conductive power lines.)

The conceptual development of counterfactual communication was based on a thought experiment proposed by Elitzur and Vaidman in 1993 (Elitzur-Vaidman Bomb Testing Scenario) \[39\]. In this quantum thought experiment (which has since been experimentally validated) \[40\], a single photon is used to detect the presence of a photosensitive bomb without interacting with and destroying the bomb in the process. This type of measurement is known as a quantum interaction-free measurement. Later, Kwiat \textit{et al.} showed how the efficiency of this interaction-free measurement could be increased arbitrarily close to unity using the quantum Zeno effect \[41\] \[42\]. This result spurred others to devise counterfactual communication systems that transmit information from point A to point B without transmitting any light, or matter/energy...
through the intervening space (SLAZ) [43]. One such system was experimentally validated in 2017 [44]. While this technique does make use of photons and open lines of potential photon transmission between point A and point B, no photons (or matter/energy) are ever transmitted between point A and point B.

Therefore, all of the photons generated at location A remain in the vicinity of location A and can be locally reabsorbed by a photocell in order to recapture their energy. The same is true for all photons generated at location B. There are no transmission losses due to photon scattering in transit between point A and point B. As previously noted, there is no fundamental limit on how much information can be transmitted per unit of energy expenditure. Accordingly, counterfactual communication (in theory) presents a means by which information could be transmitted between decentralized nodes while consuming only negligible quantities of energy. This energy expenditure could be made as low as desired through improvements to the efficiency of photon generation and photon reabsorption technologies.

Counterfactual communication thus presents a valuable tool for the efficient implementation of the E-Stablecoin network. Counterfactual communication theoretically allows for the transmission of data between nodes in the E-Stablecoin network at negligible energy costs. It also eliminates the need to transfer any matter/energy between nodes in the E-Stablecoin network. Only information is transmitted between nodes in the E-Stablecoin network. Furthermore, a counterfactual communication network may be able to piggyback on photon-based qubit transmission channels (e.g., satellite [45] and fiber optic [46]) that are already being constructed for the quantum internet [47].

5.3 Szilard Engine

The history of the Szilard engine is a long and continually unfolding one. James Clerk Maxwell first posed his riddle (now known as “Maxwell’s demon”) in 1867 [10]. This puzzle engendered a flurry of debate among physicists that lasted for over 100 years. In 1929 Leo Szilard simplified the design, making some valuable and some partially incorrect observations in the process [11]. Finally, Bennett published a resolution of the key issues in 1982 [12]. For a long time, Maxwell’s demons and Szilard engines existed only as hypothetical (though groundbreaking) thought experiments. However, in 2007 Serreli et al. developed an experimental implementation of a Maxwell’s demon using a rotoxane molecular machine [48]. Other physical demonstrations soon followed, including one using controlled manipulations of an elongated polystyrene Brownian nanoparticle suspended in a buffer solution [49], and a photonic Maxwell’s
Can a Stablecoin Be Collateralized by a Fully Decentralized, Physical Asset?

...likewise, Szilard-type engines have been implemented in laboratory settings using single electron devices and paramagnetic atoms.

In general, the maximum work that can be extracted from a Maxwell’s demon (or Szilard engine) is derivable from a generalized version of the Jarzynski equality that is applicable to feed-back controlled systems.

\[
\left\langle e^{-\beta(W-\Delta F)-(I-I_u)} \right\rangle = 1
\]  

(17)

Where \( W \) is the work done on the system, \( \Delta F \) is the change in free energy, \( I \) is the information acquired by measurements, \( I_u \) is the unavailable information, and \( \beta = \frac{1}{k_BT} \).

By applying Jensen’s inequality to Equation 17, one obtains a generalized form of the second law of thermodynamics that takes information into account.

\[
\left\langle -\beta W \right\rangle \leq -\beta \Delta F + \left\langle I \right\rangle - \left\langle I_u \right\rangle
\]  

(18)

Furthermore, if we assume that there is no change in free energy between the initial and final states, we obtain the following bound on the maximum amount of work that can be extracted given the transfer entropy, \( I_c \).

\[
W \leq k_BT I_c
\]  

(19)

Accordingly, for every usable bit of information obtained, up to \( k_BTln2 \) units of work can be extracted (if the information is efficiently exploited). Moreover, highly efficient information engines (i.e., Maxwell’s demons) that approach this upper bound have been experimentally demonstrated. In order to effectively enable the E-Stablecoin network, further advances that increase the speed, transfer entropy, and scalability of information engines will likely be required. Ongoing research into quantum, photonic, and even gambling Maxwell’s demons may pave the way forward to practical implementation.

5.4 Reversible Computing

Reversible computing serves two essential functions within the E-Stablecoin network. First, reversible computing allows Alice to extract ambient heat and convert it into work plus “waste data” using a Szilard engine (without expending energy). Second,
reversible computing allows Alice to outsource her “waste data” to Bob for erasure, so that she does not have to expend energy locally to erase it.

Historically, it was assumed that Landauer’s limit dictated a minimum bound on the amount of energy that a computer would have to dissipate to perform a computation. However, this misunderstanding has now been shown to have resulted from erroneously conflating a “computation” with an “irreversible step” [12] [61]. In reversible computing all aspects of the computation are thermodynamically reversible (isentropic) and therefore do not have a minimum energy dissipation requirement. Thus, while reversible computers can accomplish the same tasks as conventional computers, their method of operation is entirely distinct all the way from the logic gates up. Every aspect of operation must be thermodynamically reversible and therefore also logically reversible. For example, a conventional AND gate is logically irreversible. This gate has two inputs but only a single output. Therefore, information is irretrievably lost during its operation, and reversing the operation would be impossible. All reversible logic gates must be bijective. One example of a reversible logic gate is the Fredkin gate, which can be used to map any irreversible Boolean logic gate to a set of reversible gates [62].

In addition to the logic gates, the software running at all levels, and even the physical computational medium must be redesigned to be reversible. One early design of a hypothetical reversible computer is the ballistic computer [63]. This computer uses billiard balls instead of electrons as the physical medium of computation. In this design, high precision billiard balls are launched simultaneously and at identical speeds across a starting line. This launching process correlates with the inputs to the logic gate. After crossing the starting line these balls interact with reflective walls and other billiard balls within the logic gate. Finally, the locations at which the billiard balls leave the gate correlate with the output of the logic gate. The specific logic operation being executed by the gate can be adjusted by altering the starting line conditions or the reflective wall placements within the ballistic computer. This system is assumed to be frictionless and collisions between balls and between walls and balls are assumed to be perfectly elastic.

The notion of a ballistic computer is particularly intriguing as it demonstrates the viability of reversible computation at finite speeds (not infinitely slowly as required by many reversible computer proposals). The main drawback to the ballistic computer is that it is incredibly sensitive to small errors—any defects in the shape of the billiard ball or reflective walls will rapidly magnify into large computational errors. One
solution may be to use square billiard balls that are holonomically constrained to maintain their orientation. Though practical challenges remain, this idea might, for instance, be implemented using cube-shaped molecules controlled by an electric field. Other, potentially more achievable designs for reversible computing have also been proposed. These designs include reversible computers that exploit Brownian motion [15], photonics [64], quantum mechanics [65], and even RNA transcription [61].

In addition to studying the implications of reversible computing, Charles Bennett also described a process by which the value of one bit (of information) could be reversibly copied to a second preinitialized bit, or conversely by which one bit from a pair of identical bits could be reversibly erased [12]. Bennett envisioned a small, ferromagnetic ellipsoid with a single magnetic domain (in the absence of an externally applied field) that can be magnetized either parallel (“0”) or antiparallel (“1”) to the ellipse axis. In the absence of an externally applied transverse magnetic field, this particle has a bistable potential well. However, a transverse magnetic field can be applied to abolish the central barrier in the bistable potential well, creating a monostable potential well. Under these conditions, the longitudinal magnetization of the ellipsoid constitutes a “soft mode” which is very easily reoriented under the influence of a weak longitudinal magnetic field (from an external source).

More specifically, Bennett proposed a system that contains a spatially fixed transverse magnetic field (tuned in strength to abolish the bistability of a ferromagnetic particle centered within it). This fixed magnetic field is flanked on the top by a fixed reference bit (ferromagnetic particle with a set bit value of zero) and the on bottom by a fixed data bit (ferromagnetic particle holding the bit value to be copied). A movable bit (ferromagnetic particle initialized to “0”) is passed from the top (near the reference bit), into the transverse magnetic field, and then to the bottom (near the data bit), and out of the transverse magnetic field. While the movable bit is in the transverse magnetic field, it enters into a “soft mode,” wherein its resulting longitudinal magnetization is easily influenced and set by the small external longitudinal magnetic field of the closer fixed bit. When the movable bit exits the transverse magnetic field (at the bottom), its bit value (longitudinal magnetization) is locked in and identical to the value of the data bit. In this manner the moveable bit has had its magnetization (a continuous, single-valued function of position) gradually changed from agreement with the reference bit (at the top) to agreement with the data bit (at the bottom). In this manner, the data bit value is reversibly copied onto a second, preinitialized, moveable bit. Likewise, if the (now data bearing) moveable bit were taken backwards along this same path from bottom to top, it would be reversibly erased (reset to its initialized
condition by the reference bit). Therefore, one bit from a pair of identical bits can be reversibly erased. (Note that these processes do not inherently dissipate any free energy.)

Furthermore, Bennett described how a similar setup could be used to reversibly record the “waste data” from a Szilard engine (with a diamagnetic Brownian particle) [12]. For the E-Stablecoin network, it is important not only that one bit (from a pair of identical bits) can be reversibly erased, but also that the identical bits can be separated from one another by a vast distance during the erasure process (e.g., the distance between Alice and Bob). For this purpose, we propose the proceeding methodology, which follows from Bennett’s work.

Alice will transmit a copy of her “waste data” to Bob using counterfactual communication. Bob will record this data and transmit back instructions that Alice can follow to reversibly erase her locally stored “waste data.” For simplicity of description, we assume that Alice has stored her “waste data” using moveable bits in a setup similar to the one proposed by Bennett. Therefore, she can reversibly erase her “waste data” by sending each moveable bit backwards along a path that is identical (magnetically) to the path that the moveable bit encountered when she first encoded it with data from the Szilard engine.

In practice, Alice could prepare two fixed magnetic field setups. In Setup 1, Alice will flank a fixed, transverse magnetic field with a fixed “0” reference bit on the top and a fixed “0” data bit on the bottom. In Setup 2, Alice will flank a fixed, transverse magnetic field with a fixed “0” reference bit on the top and a fixed “1” data bit on the bottom. In order to reversibly erase her “waste data,” stored as moveable bits, Alice must pass each moveable bit through Setup 1 (from bottom to top) if and only if its bit value is “0.” Likewise, Alice must pass each moveable bit through Setup 2 if and only if its bit value is “1.” If a moveable bit is passed through the incorrect setup, irreversibility (and energy dissipation) will occur. Therefore, Alice must rely on Bob’s instructions to guide the process. Specifically, Bob will send Alice instructions using counterfactual communication that indicate which setup each bit should be passed through. These instructions could be actively executed in real time so that Alice does not need to store them. (Note that Bob is not allowed to expend energy to erase his locally stored “waste data” until after Alice has reversibly erased her “waste data”.) Therefore, using Bob’s instructions, Alice can reversibly erase all of her “waste data” without dissipating energy. (Note that this is only one specific design of reversible data
erasure, selected for ease of explanation. Alternative designs are expected to be more practical.)

5.5 Data Storage Capacity

As an asset-backed stablecoin, the total number of E-Stablecoin tokens that can be in circulation at any one time is limited by the size of the decentralized data storage cloud, $D$. Therefore, the total value that can be stored on the E-Stablecoin network, $V$, is limited by the size of $D$. Furthermore, physics imposes an upper bound on the number of bits of information ($I_t$) that can be stored in a finite region of space with a finite energy (or mass), the Bekenstein bound (reformulated in Equation 20) [66].

\[
I_t \leq \frac{2\pi c R m}{\hbar \ln 2}
\]  
(20)

Where $R$ is the bounded radius of the data storage device in meters, $m$ is the mass of the storage device in kilograms, $c$ is the speed of light, and $\hbar$ is the reduced Planck constant.

As an example of this bound, a spherical digital storage device with a mass of one kilogram and a radius of one meter operating at the Bekenstein bound could store the informational equivalent of approximately twenty quadrillion KWh of free energy. An E-Stablecoin network with this data storage capacity could therefore store (up to) approximately US $2$ quadrillion worth of value. However, current digital data storage technologies operate many orders of magnitude below the Bekenstein bound. Therefore, only negligible quantities of value could be stored using the digital data storage media commercially available today. In order for the E-Stablecoin network to store significant quantities of value, either digital data storage technologies will have to progress exponentially, or E-Stablecoin will have to transition to an alternative implementation wherein “waste data” can be rapidly erased and digital storage space rapidly reused. This alternative implementation would likely favor real-time free energy transfers from Bob to Alice (in the form of transmitted information) with little to no decentralized excess storage capacity. We leave it as future work to design this alternative E-Stablecoin implementation and to vet its economic structures.

One possible path forward is to make use of DNA (or RNA) data storage. On a per gram basis, DNA (or RNA) can store several orders of magnitude more data than state-of-the-art silicon-based hardware. Furthermore, DNA/RNA transcription processes are highly reversible (as with other reversible chemical reactions) and therefore operate
close to the Landauer limit in terms of energy efficiency for computation and data storage [12]. Recent experiments indicate that DNA data storage can store up to 215 Petabytes of data per gram of DNA [67]. If this data could be rewritten at the standard microprocessor frequency of 3.2 GHz, then approximately 200 kg of DNA storage could continuously transfer enough electricity to power the entire planet (approximately US $8 billion worth of value per day).

6. Conclusion

In this work we have presented the theoretical underpinnings for a new class of stablecoins (E-Stablecoin). To the authors’ knowledge this is the first proposal for a cryptocurrency that is both fully decentralized and fully collateralized by a physical asset with stable value and intrinsic utility (electricity). By making use of statistical mechanics and information theory, E-Stablecoin can store and transfer free energy between anonymous decentralized parties without requiring any centralized authorities, trusted custodians, or even conventional infrastructure.

At present, engineering and technology challenges impede the implementation of an E-Stablecoin network. Present challenges include developing efficient Szilard engines, reversible computers, and improved data storage capacity. Nonetheless, each of these challenges is also an area of active research for independent applications.

Furthermore, the mere hypothetical possibility of an E-Stablecoin network exposes assumptions that are often presumed in analyses of Bitcoin and other cryptocurrencies. For example, it is well established that creating an arbitrary number of new cryptocurrencies that are technologically identical to Bitcoin is a relatively straightforward task. On the face, this inherent cloneability (and potential proliferation) of technologically equivalent cryptocurrencies poses a threat to an asset class like Bitcoin, which relies on its scarcity to maintain its value. (Note that the price of a good cannot be established in a vacuum but instead is dependent on the availability of similar substitute goods.) A traditional counterargument to this threat is that Bitcoin has achieved runaway popularity (and adoption), which sets it apart from other cryptocurrencies and gives it a significant, if not insurmountable, advantage. However, the mere hypothetical possibility of E-Stablecoin calls into question the protections afforded by Bitcoin’s popularity moat.

The key for an asset to successfully store value over long timespans is credibility (not necessarily popularity). (Note that here assets are considered distinct from currencies, which are used regularly in transactions as a medium of exchange.) Indeed, there are a
number of rare assets that are only known, used, or appreciated in niche applications. These assets nonetheless maintain their value by virtue of their credibility in accomplishing the desired objectives, not necessarily their general popularity or brand equity.

Bitcoin has arguably leveraged its huge popularity (brand equity and adoption) into credibility. It would be a tall order for many other upstart cryptocurrencies to compete with or overtake Bitcoin strictly in terms of popularity. This represents a large and daunting activation energy that so far only Bitcoin has surmounted (first mover advantage). Nonetheless, E-Stablecoin demonstrates (even if only hypothetically) that popularity is not the only pathway by which a cryptocurrency can amass credibility. E-Stablecoin, for instance, derives credibility from the utility of its underlying asset (electricity). This process is akin to finding an alternate pathway to credibility. As if by employing a catalyst, E-Stablecoin does not have to surmount the same activation energy curve as Bitcoin in order to achieve comparable levels of credibility. E-Stablecoin and its “catalytic” shortcut to credibility thus expose a chink in the alleged armor afforded by popularity. E-Stablecoin’s “catalytic” shortcut to credibility foreshadows other shortcuts to come and the potential proliferation of cryptocurrencies, each with high levels of credibility despite only moderate popularity. Consequently, if any cryptocurrency asset leans solely on its credibility to set it apart, the entrance of other cryptocurrencies with comparable credibility (like E-Stablecoin) can pose a threat to its “unique” value proposition in the future.

Acknowledgements

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344 and was supported by the LLNL-LDRD Program under Project No. 20-ERD-014.

Corresponding Author Contact Information: mmurialdo1@gmail.com

Citations

Can a Stablecoin Be Collateralized by a Fully Decentralized, Physical Asset?


